Produkt: GDPR-sovelluskirjasto

Senast redigerat 18.09.2024

Grundläggande information

Vem tillhandahåller uppgifterna? * MET-1-1.1

Ange i vilken roll du tillhandahåller produktinformation.

Tillverkare/tjänsteleverantör

En kort presentation av produkten MET-1-2.1

Berätta kort om produkten på engelska.

Sovelluskirjasto.fi / GDPR-library EU is Due Diligence tool for software buyers. We offer you as a software vendor possibility to maintain gdpr-information of your product in the library. Platform includes also a DPIA-tool for the customers.

Presentationssida (om sådan finns) MET-1-3.1

https://sovelluskirjasto.fi

Ytterligare information (på engelska)

English version: https://www.softwarelibrary.eu

1-5 kategorier som beskriver applikationen

Plattformslösningar portaler publiceringstjänster och wikier, Systemhantering och supportprogram, Datahantering och bearbetning

1. Allmänna villkor för produkten

Finns det en åldersgräns för användare av tjänsten? GEN-1-3.1

Nej. Tjänsten har ingen åldersgräns.

Tillverkningsland / tjänsteleverantörens hemland * GEN-1-5.1

Suomi
Server is located in Germany.

ISO-certifieringar GEN-1-6.1

ISO-certifieringar som beviljats tillverkaren (27001, 27701).

Tomt/inget svar

Är det möjligt att installera en mobilapp för tjänsten? GEN-1-7.1

Tomt/inget svar

Licenstyp GEN-1-8.1

Namngiven användare

Är virtualisering möjligt? GEN-1-9.1

Beskriv hur virtualisering är möjligt och vilka resurser den kräver.

Nej

Tjänstespecifik dataskyddsbeskrivning (om sådan finns) GEN-2-1.1

https://www.sovelluskirjasto.fi/en/privacy-policy/

Tjänstens informationssäkerhetsbeskrivning (om sådan finns) GEN-2-2.1

Tomt/inget svar

Kontaktuppgifter till dataskyddsombudet GEN-2-3.1

Tomt/inget svar

Innehåller tjänsten annonser eller länkar till kommersiella tjänster? * GEN-2-4.1

Om tjänsten har kommersiellt innehåll, beskriv mer detaljerat vad och för vilken åldersgrupp det kommersiella innehållet är avsett.

Nej

Använder tjänsten cookies som användarna måste samtycka till? GEN-2-5.1

Samtycke krävs för så kallade icke-nödvändiga cookies, som kan vara relaterade till exempel spårning som utförs av tredje part. Däremot krävs inget separat samtycke för cookies som är relaterade till inloggnings- och servicefunktioner.

Nej

2. Användarhantering (slutanvändare)

Används tjänsten med personliga användarnamn? UMA-1-1.1

Om tjänsten har delar som kräver inloggning, använder de identifikationskoder och lösenord?

Ja

Har tjänstens användarhantering minst två användarnivåer: administratör och grundläggande användare? UMA-1-2.1

Minst två användarnivåer innebär att tjänsten kan ha administratörer som kan hantera andra användares id:n och åtkomsträttigheter.

Ja

Ytterligare information (på engelska)

Customers who have signed an agreement get adminstrator or basic user rights to the service.

Kan användarrättigheterna begränsas enligt de anställdas arbetsuppgifter med beaktande av de rättigheter som beviljas olika användargrupper? UMA-1-3.1

Den personuppgiftsansvarige ska kunna hantera åtkomsträttigheter till systemet i enlighet med användarnas roller och uppgifter.

Ja

Ytterligare information (på engelska)

There is possibility to limit users' access rights to the DPIA-tool.

Vilka alternativ finns det i tjänsten för att integrera användarhantering med organisationens centraliserade användarregister och enkel inloggning (SSO)? UMA-1-4.1

Ge vid behov ytterligare information om integreringsmöjligheter.

Tomt/inget svar

Ytterligare information (på engelska)

SSO integration is coming later.

Är det möjligt att logga in med användarnamn från andra tjänsteleverantörer? UMA-1-5.1

Kan jag logga in i tjänsten med Googles, Microsofts, Facebooks, Apples eller andra tjänsteleverantörers inloggningsuppgifter eller autentiseringssystem?

Nej

Är det möjligt att logga in med multifaktorautentisering (MFA)? UMA-1-6.1

Beskriv de tillgängliga alternativen för multifaktorautentisering.

Nej

Är stark autentisering av användare möjlig? UMA-1-7.1

Kan man få stark autentisering av tjänstens användare till exempel med ett elektroniskt identitetskort eller nätbankskoder?

Nej

Är det möjligt att ha gästanvändare utanför kundorganisationen eller oinloggade användare i tjänsten? UMA-1-8.1

Beskriv också hur externa användares rättigheter fastställs för åtkomst till tjänstens funktioner och lagrade data.

Ja

Ytterligare information (på engelska)

The customer can invite users outside the service to participate in the DPIA process. They get the right to modify or review an individual DPIA. They have no other rights.

Loggas all aktivitet från alla inloggade användare? * UMA-2-1.1

Den personuppgiftsansvarige ska se till att nödvändiga logguppgifter samlas in över användningen och utlämnandet av informationssystem där systemet kräver inloggning. Beskriv också hur loggarna skyddas och hur tillgången till loggarna övervakas.

Ja

Ytterligare information (på engelska)

The log information is only visible to those responsible for application development. The customer receives the log information related to their use by requesting it.

Loggas alla visningar av personuppgifter? UMA-2-2.1

Registreras t.ex. information i loggen om administratören ser andra användares uppgifter?

Ja

Är tjänstens loggdata skyddade från obehörig visning och förstörelse? UMA-2-3.1

Är tjänstens loggdata skyddade så att endast definierade ansvarspersoner kan se och radera dem?

Ja

Hur länge sparas loggdata och hur raderas de? UMA-2-4.1

Tomt/inget svar

3. Tekniskt skydd av data

Vilka integrationer (gränssnitt) finns det till systemet och hur skyddas de från utomstående? * TDP-1-1.1

Den personuppgiftsansvarige ska överföra skyddade uppgifter över ett datanät med hjälp av en krypterad eller på annat sätt säker dataöverföringsförbindelse eller -metod. Överföringen ska ske på ett sådant sätt att mottagaren på ett säkert sätt autentiseras eller identifieras innan den skyddade informationen överförs.

The service has a REST API. Use of the interface requires the conclusion of an agreement and a customer-specific password. An encrypted network connection is used for data transfer.

Hur loggas överföringar av personuppgifter via gränssnitt till underbiträden och eventuella utlämnanden till andra parter? TDP-1-2.1

Den personuppgiftsansvariges skyldighet att övervaka användningen av personuppgifter gäller även vid överföring och utlämnande av uppgifter via gränssnitt. Personuppgifter bör inte lagras i loggen om detta kan undvikas.

Tomt/inget svar

Sker all behandling av personuppgifter i tjänsten på ett sådant sätt att nätverksförbindelsen är krypterad och att användaren eller parterna i dataöverföringen är verifierade? TDP-2-1.1

När konfidentiell data överförs över datanät krypteras data med en krypteringslösning som inte har några kända sårbarheter och stöder moderna krypteringsstyrkor och -inställningar. Dessutom verifieras eller identifieras mottagaren på ett tillräckligt säkert sätt innan de uppgifter som ska skyddas överförs. Kravet gäller både funktioner som är avsedda för användare och gränssnitt som ingår i tjänsten.

Ja

Är det möjligt att använda tjänsten så att alla personuppgifter endast lagras i krypterad form? TDP-2-2.1

Kommer t.ex. personuppgifter att lagras i krypterad form i databasen i stället för i klartext? Det krävs också att dekrypteringsdata (krypteringsnycklar) hålls åtskilda från lagrade data.

Nej

Har man i tjänstens säkerhet beaktat självständig fjärråtkomst? TDP-2-3.1

Om ja, berätta hur säkerheten för tjänsten har säkerställts i en situation där tjänsten används självständigt på distans, till exempel hemifrån.

Ej besvarad

Säkerhetskopieras tjänstens datainnehåll minst en gång per dag och är det möjligt att återställa säkerhetskopian snabbt vid behov? * TDP-3-1.1

Verifierings- och återställningsprocesserna har utformats och implementerats så att de uppfyller dataskyddslagstiftningens krav på dataintegritet och tillgänglighet.

Ja

Har återställning av säkerhetskopior beskrivits och testats? TDP-3-2.1

Processen för att återställa säkerhetskopior har beskrivits och testats så att man snabbt kan återställa data från en säkerhetskopia till användning vid behov.

Ej besvarad

Kan multifaktorautentisering (MFA) framtvingas för att alla användare vid inloggning? TDP-4-2.1

Att framtvinga multifaktorautentisering innebär att tjänsten kan konfigureras så att varje användare måste aktivera den.

Nej

Installeras säkerhetsuppdateringar för tjänstens programvarukomponenter regelbundet utan dröjsmål? TDP-5-1.1

Beskriv hur hanteringen av programvaru- och korrigeringsuppdateringar är organiserad. Hur ser man till att uppdateringar fungerar säkert innan de installeras?

Ja

Har datasäkerheten auditerats av en extern part? Om ja, av vem? * TDP-5-2.1

Den personuppgiftsansvarige måste se till att lämpliga säkerhetsåtgärder har vidtagits för det informationssystem som används. Upprepas kontrollerna regelbundet?

Nej

Genomgår tjänsten regelbundna säkerhets- och sårbarhetstester? TDP-5-3.1

Informationssystemens datasäkerhet ska säkerställas genom regelbundna adekvata tester. Berätta om testningen görs internt, externt eller både och.

Ja

Ytterligare information (på engelska)

The data security of the server is regularly monitored.

Hur har den riskbaserade tillvägagångssätt och standardskyddet som krävs enligt GDPR beaktats i systemets design och dess funktioner? TDP-5-5.1

Det riskbaserade tillvägagångssättet är en princip i den allmänna dataskyddsförordningen enligt vilken de risker som är förknippade med behandlingen av personuppgifter ska bedömas och nödvändiga åtgärder vidtas för att säkerställa att behandlingen av personuppgifter är lagenlig. Dataskydd som standard innebär att endast personuppgifter som är nödvändiga för ändamålet behandlas som standard. Behandlingen av personuppgifter måste följa principen om minimering som gäller mängden personuppgifter som behandlas, behandlingens omfattning, lagringsperioden och tillgången till personuppgifter.

Tomt/inget svar

Har tjänsteleverantören rutiner för att upptäcka, anmäla och utreda personuppgiftsincidenter? TDP-5-6.1

Vänligen specificera vilka förfaranden som tillämpas.

Ej besvarad

4. Dataskydd

Vilka är syftena med behandlingen av personuppgifter? DPR-1-1.1

The name and e-mail information of the service users are collected to create user IDs.
Käyttäjän nimi ja sähköpostiosoite tarvitaan käyttäjätunnusten luomista varten.

I vilken roll placerar sig tjänsteleverantören när det gäller dataskydd? DPR-1-2.1

När det gäller de personuppgifter som tjänsteleverantören behandlar anger den om den fungerar som personuppgiftsansvarig, gemensamt personuppgiftsansvarig eller endast som personuppgiftsbiträde i kundorganisationen.

Personuppgiftsansvarig och personuppgiftsbiträde

Ytterligare information (på engelska)

Service provider is the controller of the GDPR Library itself.
Regarding the DPIA-tool, service provider position itself as a data processor.

Måste slutanvändarna ge sitt samtycke till behandling av personuppgifter i samband med tjänsten? DPR-1-3.1

Samtycke kan krävas t.ex. om (1) tjänsteleverantören inte erbjuder ett avtal för behandling av personuppgifter och de registrerades personuppgifter överförs till tjänsten, eller (2) den rättsliga grunden för behandling av personuppgifter i samband med tjänsten inte är den personuppgiftsansvariges lagstadgade skyldigheter, utan är en frivillig tilläggstjänst för vilken den personuppgiftsansvarige behöver den registrerades separata samtycke. Förklara också hur information om samtycken lagras i systemet.

Inget svar

Är det möjligt att göra kundorganisationens namn och en länk till dess egen dataskyddsbeskrivning synlig för användare i tjänsten? DPR-1-4.1

Användare av tjänsten ska alltid kunna se vem som är personuppgiftsansvarig för tjänsten och borde informera om behandlingen av personuppgifter.

Nej

Har tjänsteleverantören tillgång till personuppgifter som kundorganisationen lagrar? * DPR-1-5.1

Lagras personuppgifterna i tjänsten i ett format som är tillgängligt för tjänsteleverantören? Finns det andra funktioner i tjänsten som leder till att leverantören får tillgång till personuppgifter?

Ja

Ytterligare information (på engelska)

The service provider creates user accounts for the software vendor's and customer's employees and manages them (controller).
As a data processor, the service provider has access to the data to be entered into the DPIA tool.

Uppstår det i och med användningen av tjänsten ett register där tjänsteleverantören är gemensamt personuppgiftsansvarig med kundorganisationen? DPR-1-6.1

Gemensamt personuppgiftsansvar föreligger när aktörerna gemensamt fastställer ändamålen och medlen för behandlingen av personuppgifter och delar på den personuppgiftsansvarets ansvar. I enlighet med artikel 26 i GDPR ska gemensamt personuppgiftsansvariga genom ömsesidig överenskommelse fastställa ansvaret för att uppfylla dataskyddsskyldigheterna.

Nej

Har tjänsteleverantören en uppdaterad förteckning över underbiträden av personuppgifter, där det framgår namn, plats, syfte med behandlingen och eventuell överföringsgrund utanför EU/EES-området? * DPR-1-8.1

Den personuppgiftsansvarige ska informeras om alla personuppgiftsbiträden som behandlar personuppgifter i samband med tjänsten. Endast personuppgiftsbiträden som vidtar tillräckliga skyddsåtgärder får anlitas för behandlingen.

Ja

Länk till lista över underbiträden (om sådana finns) DPR-1-9.1

Tomt/inget svar

Ytterligare information (på engelska)

As a sub-processor acts:
* Innowise Oy (VAT 1919750-1), DPA has been signed.
* AtWise LLC (VAT 4024020507382), DPA has been signed, DPIA data is not shared.

* Ilona IT is itself the data controller for the GDPR application library, and then AtWise and Innowise are the processors.
* Client is the data controller for the data of the DPIA tool and then Ilona IT is the personal data processor and only Innowise is the sub-processor. AtWise does not have access rights to the content and data of the DPIA tool, and therefore does not act as a sub-processor in that respect.

Behandlar tjänsteleverantören eller något av dess underbiträden personuppgifter utanför EU/EES? DPR-1-10.1

Tjänsteleverantören har identifierat internationella överföringar av personuppgifter utanför EU/EES i samband med sin verksamhet och de överföringsgrunder som används för dem, och har säkerställt att lagstiftningen i det tredje landet eller de ytterligare skyddsåtgärder som tillämpas garanterar en sådan skyddsnivå för de uppgifter som överförs som väsentligen motsvarar den skyddsnivå som tillhandahålls av EU:s dataskyddslagstiftning.

Ja

Ytterligare information (på engelska)

In Macedonian co-operation firm AtWise LLC (VAT: 4024020507382), DPA has been signed, DPIA data is not shared.

Om personuppgifter behandlas utanför EU/EES, på vilken grund överförs personuppgifterna? DPR-1-11.1

För överföring av personuppgifter utanför EU/EES krävs en överföringsgrund i enlighet med den allmänna dataskyddsförordningen. För mer information: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

Standardklausuler som antagits av kommissionen (artikel 46:2c och artikel 46:2d)

Ytterligare information (på engelska)

Personal data is primarily processed within the EU/EEA area only. Personal data may, however, be transferred outside the EU/EEA especially if a services provider we use is located outside the EU/EEA.

If personal data were to be transferred outside the EU/EEA to a country that is not included in the EU Commission's decision on an adequate level of data protection, we will make sure that the processing, transfer and storage of your data is carried out on the grounds required by law and with adequate protection mechanisms, such as using the standard contract clauses confirmed by the EU Commission.

Kan personuppgifter överföras till icke-säkra tredjeländer? * DPR-1-12.2

Med icke-säkra länder avses länder vars myndigheter kan ha tillgång till personuppgifter eller vars lagstiftning inte garanterar en nivå av dataskydd som motsvarar den som som EU:s dataskyddslagstiftning ger.

Nej

I vilka länder finns tjänsteleverantörens servrar? DPR-1-13.1

Ange också om platsen för de servrar som används kan väljas.

Germany

Vilka personuppgifter behandlar tjänsteleverantören? * DPR-2-1.1

Förteckning över kategorier av registrerade och typer av personuppgifter som ska behandlas.

Company name (employer)
Name of the person
Email address
Username and password
Log history of data entries and edits in the service, mainly: (1) who entered/edited data, (2) entries/edits made, (3) time stamp – this data is collected to ensure reliability of data in the service
Customary contact and billing details required for billing and invoicing paid services
Customary correspondence with users
Possibly information entered by the customer into the DPIA-tool.

Är tjänsten också avsedd för behandling av särskilda personuppgifter (t.ex. hälsouppgifter)? * DPR-2-2.1

Är tjänsten uttryckligen avsedd för att behandla specifika personuppgifter i den mening som avses i EU:s allmänna dataskyddsförordning?

Nej

Kan de obligatoriska och frivilliga fälten som är relaterade till användare definieras av administratören? DPR-2-3.1

Ja

Erbjuder tjänsteleverantören användarna omfattande information om behandlingen av personuppgifter i tjänsten? DPR-2-4.1

Ja

Vilka metoder finns för att säkerställa att uppgifterna inte används för andra ändamål? DPR-2-6.1

Tjänsteleverantören får endast behandla personuppgifter för de ändamål som anges i DPA-avtalet och de instruktioner som ges av den personuppgiftsansvarige.

DPA:s with sub-processors and customers

Har tjänsten en funktion för att pseudonymisera personuppgifter? DPR-2-7.1

Nej

Kan man separat be användarna om deras samtycke till behandling av vissa personuppgifter (t.ex. personbeteckning eller särskilda kategorier av personuppgifter)? DPR-2-8.1

Förklara mer i detalj för vilka personuppgifter och ändamål samtycke kan begäras separat från användaren. Till exempel kan behandling av personbeteckningar och särskilda kategorier av personuppgifter (t.ex. hälsouppgifter) kräva uttryckligt samtycke, om den personuppgiftsansvarige inte har laglig rätt att behandla dem.

Nej

Ytterligare information (på engelska)

Personal identification number or special personal data are not collected.

Bearbetar tjänsten data i stor skala? DPR-2-9.1

Vid bedömningen av omfattningen rekommenderas att man tar hänsyn till antalet registrerade, mängden

personuppgifter som ska behandlas, behandlingens varaktighet och den geografiska omfattningen.

Nej

Kan profilering, poängsättning eller utvärdering av individer anknyta till tjänstens funktioner? DPR-2-10.1

Kopplat till behovet av en konsekvensbedömning.

Nej

Can the service involve the processing of location data? * DPR-2-11.1

Kopplat till behovet av en konsekvensbedömning.

Nej

Kan personuppgifternas lagringstider eller kriterir för dessa fastställas i tjänsten? * DPR-2-12.1

Det ska vara möjligt att definiera behandlingstiden för personuppgifter.

Nej

Ytterligare information (på engelska)

The customer must inform the service provider when the data of its employees must be deleted. When the contract ends the data will be deleted automatically.
When a user or customer organization is deleted, any log file associated with the user is also deleted (administrators).

Kan användarnas personuppgifter anonymiseras istället för att raderas? DPR-2-13.1

Nej

Står omfattningen och längden av behandlingen av personuppgifter i proportion till de fördelar som eftersträvas? DPR-3-3.1

Proportionalitet innebär till exempel att applikationen inte lagrar onödig information om användarnas enheter och att användarna inte ombeds lämna ut information som inte tydligt krävs för att använda tjänsten.

Ja

Kan användarna se all data som lagras om dem? DPR-4-2.1

Nej

Ytterligare information (på engelska)

The user cannot directly see the log data stored about their activity.

Kan användare ladda ner eller överföra data som de har lagrat i en annan tjänst, eller importera data från ett annat system? DPR-4-3.1

Om behandlingen av personuppgifter grundar sig på samtycke eller ett avtal bör användarna ha möjlighet att ladda ner sina uppgifter i ett allmänt använt filformat. Förklara också vilka tekniska möjligheter användarna har att överföra uppgifter till ett annat system eller att importera uppgifter från ett annat system.

Nej

Ytterligare information (på engelska)

The amount of personal data is minimal.

Hur och när raderas personuppgifter? *

DPR-4-4.1

Det ska vara möjligt att definiera behandlingstiden för personuppgifter.

The customer must inform the service provider when the data of its employees must be deleted during the contract. When the contract ends the data will be deleted automatically.
When a user or customer organization is deleted, any log file associated with the user is also deleted (administrators).

Om den registrerade utövar sin rätt att begränsa behandlingen av sina personuppgifter, vilka tekniska medel används för att säkerställa att begränsningen genomförs?

DPR-4-5.1

Registrerade har rätt att begära att behandlingen av deras personuppgifter begränsas om de ifrågasätter uppgifternas riktighet eller behandlingens laglighet. Behandlingen av uppgifter ska också begränsas om den registrerade motsätter sig att de behandlas för ett visst ändamål (t.ex. marknadsföring) eller helt och hållet.

The registered person can request the deletion of their user ID and refuse customer communication.

Hur säkerställer man att de personuppgifter som behandlas är korrekta?

DPR-5-1.1

Beskriv hur man säkerställer att de uppgifter som behandlas är korrekta, att de kontrolleras regelbundet och att eventuella felaktiga uppgifter uppdateras utan dröjsmål.

If the person himself/ herself informs the service provider or the regularly sent customer letter is returned to the service provider, the reason will be checked and, if necessary, the person will be removed from the user register or the information will be changed.

Fattas automatiserade beslut i tjänsten och i så fall på vilka grunder?

DPR-6-1.1

Förklara grunderna för eventuella automatiserade beslut. Automatiserat beslutsfattande är tillåtet om det är nödvändigt för att ingå eller fullgöra ett avtal, om det är tillåtet enligt tillämplig lag eller om det grundar sig på den registrerades samtycke.

Nej

Hur informeras de registrerade om automatiserat beslutsfattande?

DPR-6-2.1

Beskriv hur den registrerade informeras om automatiserat beslutsfattande och de metoder som används i det.

Tomt/inget svar

Hur beskrivs slutsatser som baserar sig på automatiserat beslutsfattande för den registrerade?

DPR-6-3.1

De registrerade bör få information om de har placerats i vissa grupper eller segment på basis av automatiserat beslutsfattande och profilering. Det kan också vara fråga om en klassificering som beskriver den registrerades verksamhet eller intressen.

Tomt/inget svar

5. DPA-avtal

Är det möjligt att ingå ett avtal med underleverantören om behandling av personuppgifter (DPA)? * DPA-1-1.1

Den personuppgiftsansvarige ska ingå ett avtal med personuppgiftsbiträdet som uppfyller kraven i EU:s dataskyddsförordning.

Ja; ett standardiserat DPA-avtal

Länk till standardmall för DPA-avtalet (om tillämpligt) DPA-1-2.1

https://ilonait.adobeconnect.com/dpa_fi/

Ytterligare information (på engelska)

DPA in Finnish. Ask the English version: soili@ilonait.fi

Definieras de personuppgifter som behandlas i DPA-avtalet? DPA-1-3.1

Ja

Definieras personuppgifternas behandlingsändamål i DPA-avtalet? DPA-1-4.1

Personuppgiftsbiträdet får endast behandla personuppgifter för de ändamål som anges i DPA-avtalet och i den personuppgiftsansvariges anvisningar.

Ja

Kan man i samband med DPA-avtalet ge anvisningar som tjänsteleverantören ska beakta vid behandling av personuppgifter? DPA-1-5.1

Den personuppgiftsansvarige ska ge anvisningar om behandlingen av personuppgifter och se till att personuppgifterna behandlas i enlighet med dem.

Nej

Framgår det av DPA-avtalet att tjänsteleverantören kommer att upprätthålla konfidentialitet för sina anställda? DPA-1-6.1

DPA-avtalet ska säkerställa att behandlingen av personuppgifter är konfidentiell.

Ja

Framgår det av DPA-avtalet att tjänsteleverantören tillåter den personuppgiftsansvarige att övervaka och granska? DPA-1-7.1

Krav på DPA-avtalet i EU:s allmänna dataskyddsförordning.

Ja

Har tjänsteleverantören en utsedd kontaktperson för dataskyddsfrågor? DPA-1-8.1

Ja

Ytterligare information (på engelska)

soili@ilonait.fi

Innehåller DPA bestämmelser om radering av uppgifter? DPA-1-9.1

När behandlingen av personuppgifter upphör ansvarar tjänsteleverantören för att radera eller återsända uppgifterna till den personuppgiftsansvarige.

Ja

Använder tjänsteleverantören användarnas personuppgifter för andra ändamål än de som är relaterade till drift och underhåll av tjänsten? DPA-1-10.1

Tjänsteleverantören får inte använda personuppgifter för andra ändamål än de som är direkt kopplade till den tjänst som tillhandahålls, såsom dess funktioner och underhåll. Användning av uppgifter för ändamål som leverantörens egen produktutveckling eller för tredjepartsändamål kan vara problematisk.

Nej

Säkerställs efterlevnaden av EU:s allmänna dataskyddsförordning (GDPR) och implementeringen av lämpliga skyddsåtgärder i DPA-avtalet om underbiträden används för behandling av personuppgifter? DPA-2-1.1

Tjänsteleverantören får endast anlita personuppgiftsbiträden som vidtar tillräckliga skyddsåtgärder i enlighet med EU:s allmänna dataskyddsförordning. Beskriv hur underbiträden utvärderas och hur deras verksamhet övervakas.

Ja

Ytterligare information (på engelska)

DPA is signed.

Underbiträden enligt DPA-avtalet eller länk till förteckningen över underbiträden (om tillämpligt) DPA-2-2.1

As a sub-processor acts:
* Innowise Oy (VAT 1919750-1), DPA has been signed.
* AtWise LLC (VAT 4024020507382), DPA has been signed, DPIA data is not shared.

* Ilona IT is itself the data controller for the GDPR application library, and then AtWise and Innowise are the processors.
* Client is the data controller for the data of the DPIA tool and then Ilona IT is the personal data processor and only Innowise is the sub-processor. AtWise does not have access rights to the content and data of the DPIA tool, and therefore does not act as a sub-processor in that respect.

Uppfyller tjänsteleverantören kraven i dataskyddsförordningen när det gäller ändringar av underbiträden? DPA-2-3.1

Enligt artikel 28.2 i GDPR: "Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar."

Ja

Förbinder sig tjänsteleverantören att utan dröjsmål anmäla alla personuppgiftsincidenter? DPA-3-1.1

Tjänsteleverantören ska skriftligen underrätta den personuppgiftsansvarige om en personuppgiftsincident utan onödigt dröjsmål efter att ha fått kännedom om den.

Ja

Har tjänsteleverantören ett avtalat förfarande för att rapportera personuppgiftsincidenter? DPA-3-2.1
Tjänsteleverantören ska dokumentera alla personuppgiftsincidenter och fastställa rutiner för hur de ska rapporteras till den personuppgiftsansvarige.

Ja

Förbinder sig tjänsteleverantören att utan dröjsmål tillmötesgå begäran som om personuppgifter? DPA-3-3.1
Tjänsteleverantören ska åta sig att snabbt svara på förfrågningar från den personuppgiftsansvarige. En sådan begäran kan t.ex. vara att radera eller avbryta behandlingen av personuppgifter.

Ja

Behandlar personuppgiftsbiträdet eller något av dess underbiträden personuppgifter utanför EU/EES? * DPA-4-1.1
Tjänsteleverantören ska identifiera internationella överföringar av personuppgifter utanför EU/EES som hänför sig till dess verksamhet och de överföringsgrunder som används för dem, samt se till att lagstiftningen och praxisen i det tredje landet garanterar en skyddsnivå för personuppgifter som väsentligen motsvarar nivån i EU:s allmänna dataskyddsförordning.

Ja

Ytterligare information (på engelska)

DPA is signed.

Om personuppgifter behandlas utanför EU/EES, på vilken grund överförs personuppgifterna? DPA-4-2.1
För överföring av personuppgifter utanför EU/EES krävs en överföringsgrund i enlighet med EU:s dataskyddsförordning. För mer information: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

Standardklausuler som antagits av kommissionen (artikel 46:2c och artikel 46:2d)

Om EU-kommissionens standardavtalsklausuler (SCC) används som grund för överföring av personuppgifter, vilka SCC är det då fråga om? DPA-4-3.1
För ytterligare information och standardavtalsklausuler för överföring av uppgifter till tredjeländer (artikel 46), besök kommissionens webbplats: EU Standard Contractual Clauses https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Överföring av personuppgifter från en personuppgiftsansvarig till ett personuppgiftsbiträde

---

Kan personuppgifterna lämnas ut till myndigheter i tredje land? * DPA-4-4.1
Om personuppgifter överförs utanför EU/EES till ett land där myndigheterna kan ha tillgång till personuppgifterna, måste den personuppgiftsansvarige bedöma om ytterligare skyddsåtgärder behövs.

Nej

Har tjänsteleverantören dokumentation som hjälper till med konsekvensbedömning av dataöverföringar (transfer impact assessment, TIA) i situationer där data överförs utanför EU/EES? DPA-4-5.1

Om personuppgifter överförs utanför EU/EES bör den personuppgiftsansvarige bedöma om ytterligare skyddsåtgärder är nödvändiga. Rekommendation 1/2020 om åtgärder för att komplettera instrument för överföring av uppgifter för att säkerställa den skyddsnivå som garanteras för personuppgifter i EU: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Ja

Ytterligare information (på engelska)

Organizational protective measures: e.g. limiting the persons who have access to the data and minimizing the data, i.e. not sharing or processing more data than is necessary. DPIA-data is not shared outside EU.

Contract-based: written contracts, in which e.g. conditions regarding confidentiality and information security obligations, to which the contracting party must commit.

Om uppgifter överförs utanför EU/EES, vilka ytterligare skyddsåtgärder tillämpas? DPA-4-6.1

Organizational protective measures: e.g. limiting the persons who have access to the data and minimizing the data, i.e. not sharing or processing more data than is necessary.
Contract-based: written contracts, in which e.g. conditions regarding confidentiality and information security obligations, to which the contracting party must commit.